IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): ~~Method~~ A method for the authentication of data communicated from [[a]] an originator to a destination, comprising:

~~wherein~~ using a keyed hashing technique ~~is used~~, according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function;

transmitting ~~and~~ the data ~~are transmitted~~ together with ~~the~~ a digest of the hash function from the originator to the destination,

~~characterized in that~~

wherein the data comprises temporal validity information representing the temporal validity of the data;

~~the originator receives~~receiving, at the originator, an acknowledgement key from the destination, wherein the acknowledgement key includes a time stamp; and

verifying, at the originator, ~~verifies~~ the acknowledgment key on the basis of the time stamp and the previously stored temporal validity information,

wherein the keyed hashing technique uses random data that is stored by the destination in a table during the temporal validity of the data.

Claim 2 (Currently Amended): ~~Method~~ The method according to claim 1,

~~characterized in that~~ wherein the temporal validity information can be defined by the originator.

Claim 3 (Currently Amended): ~~Method~~ The method according to claim 1,

~~characterized in that~~ wherein the data comprises random data which are unique for a time span defined by the temporal validity information.

Claim 4 (Currently Amended): ~~Method~~ The method according to claim 1, ~~characterized in that~~ wherein the data is a login key for a communication setup.

Claim 5 (Currently Amended): ~~Method~~ A method for the authenticated transmission of messages, comprising the following communication setup steps:

- generating a login key by a keyed-hashing method on the basis of random data, temporal validity information, and a private key,

- transmitting the login key from an originator to a destination, and

- verifying the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest on the destination side; and

comprising the following acknowledgement steps:

in case the verification of the authenticity and the temporal validity of the login key is positive,

- generating an acknowledgment key by a keyed-hashing method on the basis of second random data and the private key, wherein the acknowledgement key includes a time stamp,

- transmitting the acknowledgment key from the destination to the originator, and

- verifying the acknowledgment key by the originator, including checking the acknowledgement key on the basis of the time stamp and the previously stored temporal validity information whether the acknowledgment key is still valid,

wherein the keyed-hashing technique uses random data that is stored by the destination in a table during the temporal validity of the data.

Claims 6-7 (Canceled).

Claim 8 (Currently Amended): ~~Method~~ The method according to claim 5, ~~furthermore~~ further comprising the following message transmission steps:

in case the verification of the acknowledgment key is positive,

- extracting the second random data from the acknowledgment key,

- generating a message by a keyed-hashing method on the basis of the second random data, message data, and the private key,

- transmitting the message from the originator to the destination, and

- verifying the message by the destination.

Claim 9 (Currently Amended): ~~Method~~ The method according to claim 8, wherein ~~characterized in that~~

the message ~~furthermore~~ comprises a time stamp, and

the step of~~when~~ verifying the message ~~it is checked~~ includes checking on ~~the basis of~~ the time stamp of the message and the temporal validity information to determine whether the message is still valid.

Claim 10 (Currently Amended): A storage medium storing a software program product,

~~characterized in that~~

the software program product implements, when loaded into a computing device of a distributed system, ~~a~~ the method according to claim 5.

Claim 11 (Currently Amended): ~~Distributed~~ A distributed system comprising: ~~for communicating authenticated data from a~~

an originator configured to communicate authenticated data to a destination;[[,]]

the system designed for a keyed hashing technique, according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function, and the data are transmitted together with the digest of the hash function from the originator to the destination,

~~characterized in that~~

wherein the data comprises temporal validity information representing the temporal validity of the data;

the originator receives an acknowledgement key from the destination, wherein the acknowledgement key includes a time stamp; and

the originator verifies the acknowledgment key on the basis of the time stamp and the previously stored temporal validity information,

wherein the keyed hashing technique uses random data that is stored by the destination in table during the temporal validity of the data.

Claim 12 (Currently Amended): ~~Distributed~~ The distributed system according to claim 11, wherein

~~characterized in that~~

the originator is designed to define the temporal validity information.

Claim 13 (Currently Amended): ~~Distributed~~ The distributed system according to claim 11, wherein

~~characterized in that~~

the data comprises random data which are unique for a time span defined by the temporal validity information.

Claim 14 (Currently Amended): ~~Distributed~~ The distributed system according to claim 11, wherein

~~characterized in that~~

the data is a login key for a communication setup.

Claim 15 (Currently Amended): ~~Distributed~~ A distributed system for the authenticated transmission of messages, comprising:

- an originator designed to generate a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key, wherein the login key includes a keyed hashing digest; and

- a network for transmitting the login key from the originator to a destination, wherein the destination is designed to verify the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest;

wherein the destination is designed to generate an acknowledgment key by a keyed-hashing method on the basis of second random data and the private key and to transmit the acknowledgment key to the originator in case the verification of the authenticity and the temporal validity of the login key is positive, and the acknowledgement key includes a time stamp,

the originator is designed to verify the acknowledgment key, including checking on the basis of the time stamp and the previously stored temporal validity information whether the acknowledgment key is still valid, and

the key hashing technique uses random data that is stored by the destination in a table during the temporal validity of the data.

Claims 16-17 (Canceled).

Claim 18 (Currently Amended): ~~Distributed~~ The distributed system according to claim 15, wherein

~~characterized in that~~

the originator is ~~designed~~ configured to extract the second random data from the acknowledgment key in case the verification of the acknowledgment key is positive, generate a message by a keyed-hashing method on the basis of the second random data, message data and the private key, and transmit the message to the destination, and

the destination is ~~designed~~ configured to verify the message.

Claim 19 (Currently Amended): ~~Distributed~~ A distributed system according to claim 18, wherein

~~characterized in that~~

the message ~~furthermore~~ comprises a time stamp, and

~~when verifying the message,~~ the destination checks, when verifying the message, on ~~the basis of~~ the time stamp of the message and the temporal validity information to determine whether the message is still valid.

Claim 20 (Currently Amended): ~~Method~~ The method according to claim 1,

~~characterized in that~~ wherein the data is a message.

Claim 21 (Currently Amended): ~~Distributed~~ The distributed system according to claim 11,

~~characterized in that~~ wherein the data is a message.

Claim 22 (Currently Amended): ~~Method~~ The method according to claim 1, wherein the ~~originator verifying the acknowledgment key on the basis of the time stamp and the previously stored temporal validity information~~step of verifying includes

calculating an absolute value difference between an acknowledgment universal time and a current time of the originator.

Claim 23 (Currently Amended): ~~Method~~ The method according to claim 22, further comprising:

comparing the absolute value difference to the temporal validity of the acknowledgment key.

Claim 24 (Currently Amended): ~~Method~~ The method according to claim 23, further comprising:

authenticating the acknowledgment key when the result of the comparison indicates the absolute value difference is less than the temporal validity of the acknowledgment key.

Claim 25 (Canceled).

26 (New): The method according to claim 1, further comprising:

searching, upon reception of data and corresponding random data, said table for an entry identical to said received random data, said searching being performed by the destination.

27 (New): The method according to claim 2, further comprising:

aborting the authentication in case an entry corresponding to the received random data was found in said table, said aborting being performed by the destination.